Amendments to the Specification:

Please replace paragraphs 43 (which is the carryover paragraph on from page 13 to page 14), 61 (which is the carryover paragraph on from page 19 to page 20), and 63 (which is the paragraph on page 20 from lines 15 to 31), with the correspondingly numbered paragraphs listed below, each marked up to show changes from the prior version.

[0043] As illustrated in FIG. 6, the I/O element 60 comprises a processor 62 that includes a flow classification block 64, a layer 4 termination block 66 and a layer 4 segmentation block 68 which together are logically equivalent to the layer 4 port 144 and layer 4 socket 142 of FIG. 5. The flow classification block 64 classifies packets received from a packet switched network into separate flows of packets based upon the flow identifiers attached to the packets, the flow identifiers including the source layer 3 address, the source layer 4 port, the destination layer 3 address, the destination layer 4 port and the layer 4 identifier (i.e. UDP or TCP etc.). Each flow of packets corresponds to a different stream of data. The layer 4 termination block 66 performs well-known reconstituting of the data stream by removing the packet overhead from the data, re-ordering the data within the received packets and requesting re-transmissions of packets that have been lost. The output from the layer 4 termination block 66 are substreams including correctly ordered portions of the overall data stream. The layer 4 segmentation block 68 performs well-known segmentation operations of incoming data from the stream fabric 70 and outputs packets including the segmented data along with layer 3 and layer 4 headers to a packet switched network

[0061] FIG. 11 illustrates the block diagram of FIG. 6 with the signalling depicted for a scenario in which encrypted data is detected within the data stream by the content processing element 80. In this case, the operation of the stream processing node 50 is identical to that described above for FIG. 7 until the content processing element has completed its analysis of the copied portion of the stream queue SQ2. In this case, the content processing element 80 determines that the data within the stream is encrypted and, as indicated by signal 714, requests rescheduling of the stream queue SQ1 to the first application processing element 90, which in this scenario has a decryption algorithm and therefore is a decryption processing element. The stream queue controller 72 then modifies the consumer attributes for the stream queue SQ1 such that the consumer is set as the application processing element 90 and

initiates a pop of data from the stream queue SQ1 to the processing element 90 as indicated by signal 716.

[0063] Turning to FIG. 11, the application processing element 90, acting as a decryption processing element, receives portions of the data within stream queue SQ1 and outputs decrypted versions of the data stream into stream queue SQ3 as indicated by signal 718. In this scenario, the application processing element 90 initiated the stream queue SQ3 such that the initial consumer was chosen to be the content processing element 80. In this case, as described previously, a copy of the data within the stream queue SQ3 is copied to the content processing element 80 as indicated by signal 720. After analysing this data, the content processing element 80 then sends instructions to the stream queue controller by signal 714. In the scenario depicted in FIG. 11, the content processing element 80 determines the decrypted data stream includes a URL that should be used to properly route the data stream similar to the scenario of FIG. 7. This results in the rescheduling of the stream queue SQ3 to the I/O element 60, the popping of portions of the data within the stream queue SQ3 to the I/O element 60 as indicated by signal 722 and the eventual outputting of packets 724 corresponding to the decrypted data stream to the packet switched network.